IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:
Kinderknecht, et al.

Application No. 10/829,499
Filed: April 22, 2004

Examiner: Tuan A. Vu
Art Unit: 2193

Confirmation No.: 6946

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CLAIM AMENDMENTS TO ENABLE EXAMINER'S AMENDMENT

Sir:

In response to a telephone call from Examiner Vu, the following amendments are proposed for entry by way of an Examiner's Amendment.

Amendments to the claims begin on page 2.

Remarks begin on page 6.

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A system for controlling an application process comprising:

first computer means associated with a secured computing environment, the first computer means for recognizing a request for access by a client computer to resources of the secured computing environment, the client computer being remote from the secured computing environment, for pushing an access policy to the client computer, the access policy identifying resources in the secured computing environment authorized for access by the client computer, and for providing to the client computer an injector to be stored on the client computer, the injector operable to inject redirect code into a memory space used by an application process executing on the client computer, the application process for communicating with the resources of the secured computing environment for which access is requested; and

a library of redirect functions operable to be referenced by the redirect code during execution of the application process, wherein the redirect code is operable to (i) intercept at least one function call made by the application process to access secured data associated with the resources of the secured computing environment for which access is requested, and (ii) execute at least one of the redirect functions in place of the at least one intercepted function call so as to enable the application process, executing at the first computing device, to access the secured data,

wherein the first computer means comprises a firewall securing all access to the resources in the secured computing environment.

2. (Cancelled)

3. (Previously Presented) The system, as set forth in claim 1, wherein the at least one function call comprises a socket function call.

4. (Original) The system, as set forth in claim 1, wherein the library of redirect functions comprises a dynamic link library.

5. (Cancelled)

6. (Currently Amended) The system, as set forth in claim ~~5~~ 1, wherein the application process comprises an application operable to communicate with the secured computing environment resources using an Internet transport protocol, the redirect code, and the redirect functions.

7. (Original) The system, as set forth in claim 1, wherein the application process comprises an email application.

8. (Original) The system, as set forth in claim 1, wherein the application process comprises a web browser application.

9. (Original) The system, as set forth in claim 1, wherein the application process comprises a file transfer application.

10. (Currently Amended) A method for controlling an application process comprising:

pushing, from first computer means associated with a secured computing environment~~, an injector~~ to a first computing device remote from the secured computing environment and enabled to execute the application process, (i) an access policy specifying resources accessible by a user associated with user information received and authenticated at the first computer means and (ii) an injector, said pushing being responsive to a request for access by the first computing device to a resource of the secured computing environment; and

at the first computing device, starting an execution of the application process, the application process for communicating with the resource of the secured computing environment, interrupting the execution of the application process, injecting, via the injector, a redirect code into a memory space of the first computing device used by the application process, and executing the redirect code in the application process to reference a redirect library of redirect functions so that upon resuming the execution of the application process, the redirect code is operable to (i) intercept at least one function call made by the application process to access secured data at the resource of the secured computing environment for which access is requested, and (ii) execute at least one redirect function in place of the at least one function call so as to enable the application process, executing on the first computing device, to access the secured data,

wherein said first computer means comprises a firewall.

11. (Cancelled)

12. (Previously Presented) The method, as set forth in claim 10, wherein starting and interrupting the execution of the application process comprises starting the execution of the application process using a debug option, and catching an exception thrown by the application process; and wherein injecting the redirect code comprises locating memory space used by the application process, injecting the redirect code into the memory space used by the application process, and setting an instruction pointer to the redirect code.

13. (Previously Presented) The method, as set forth in claim 10, wherein starting and interrupting the execution of the application process comprises starting the execution of the application process using a suspend option; and wherein injecting the redirect code comprises creating memory space in the application process, injecting the redirect code into the memory space of the application process, and setting an instruction pointer to the redirect code.

14. (Previously Presented) The method, as set forth in claim 10, wherein starting and interrupting the execution of the application process comprises starting the execution of the application process using a suspend option; and wherein injecting the redirect code comprises creating memory space in the application process, injecting the redirect code into the memory space of the application process, and using a create remote thread function to execute the redirect code.

15. (Original) The method, as set forth in claim 10, wherein executing the redirect code comprises:

loading the redirect library of redirect functions;

determining a location of an import table replacement function in the redirect library; and executing the import table replacement function.

16. (Original) The method, as set forth in claim 15, wherein loading the redirect library of redirect functions comprises loading a dynamic link library.

17. (Previously Presented) The method, as set forth in claim 15, wherein executing the import table replacement function comprises:

searching an import table of the application process for the at least one function call; and

modifying the at least one function call to reference one or more redirect functions in the redirect library.

18. (Previously Presented) The method, as set forth in claim 15, wherein executing the import table replacement function comprises:

searching dynamic link libraries of the application process for the at least one function call; and

modifying the at least one function call to reference one or more redirect functions in the redirect library.

19. (Cancelled)

20. (Currently Amended) The method, as set forth in claim ~~19~~ 10, wherein intercepting the at least one function call comprises intercepting at least one socket function call.

21. (Currently Amended) The method, as set forth in claim ~~19~~ 10, ~~wherein the first computer means comprises a firewall and~~ further comprising executing redirect functions to enable secured access by the first computing device to a plurality of resources of the secured computing environment via the firewall.

22 - 33. (Cancelled)

REMARKS

Entry of the foregoing amendments by way of Examiner's amendment is respectfully requested.

Responsive to a telephone call from Examiner Vu on September 28, 2009, the subject matter from former claim 5 has been incorporated in claim 1, as amended. Likewise, subject matter from former claim 19 and from claim 21 has been incorporated in claim 10. No new matter is being introduced by these amendments.

Please charge our Deposit Account No. 19-3140 for any deficiencies of fees.

Respectfully submitted,
SONNENSCHEIN NATH & ROSENTHAL LLP

Date: September 28, 2009

/Tarek N. Fahmi/
Tarek N. Fahmi
Reg. No. 41,402

P.O. Box 061080
Wacker Drive Station
Willis Tower
Chicago, IL 60606-1080
650-798-0320